Mr. Chairman and Members of the Subcommittee:

Drinking water utilities across the country have long been recognized as potentially vulnerable to terrorist attacks of various types, including physical disruption, bioterrorism, chemical contamination, and cyber attack. Damage or destruction by terrorists could disrupt not only the availability of safe drinking water, but also the delivery of vital services that depend on these water supplies, such as fire suppression. Such concerns were greatly amplified by the September 11, 2001, attacks on the World Trade Center and the Pentagon and then by the discovery of training manuals in Afghanistan detailing how terrorist trainees could support attacks on drinking water systems.

Congress has since committed significant federal funding to assist drinking water utilities—with over $140 million appropriated from fiscal year 2002 through fiscal year 2004—to help systems assess their vulnerabilities to terrorist threats and develop response plans. As significant as these funds are, drinking water utilities are asking the federal government to support efforts that go beyond the *planning* for upgrading drinking water security to the actual *implementation* of security upgrades. Consequently, at the request of the Senate Committee on Environment and Public Works, we examined (1) the key security-related vulnerabilities affecting the nation's drinking water systems; (2) the criteria that experts believe should be used to determine how federal funds are allocated among recipients to improve their security, and the methods that should be used to distribute these funds; and (3) specific activities that experts believe the federal government should support to improve drinking water security. My testimony is based on our October 2003 report entitled, *Drinking Water: Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security.*

To prepare our October 2003 report on these issues, we assembled a panel of nationally recognized experts. In selecting members for the expert panel, we sought individuals who were widely recognized as possessing expertise on one or more key aspects of drinking water security. We also sought to achieve balance in representation from key

federal agencies, key state or local agencies, key industry and nonprofit organizations, and water utilities of varying sizes.

In summary:

- Our expert panel identified several key physical assets as the most seriously vulnerable to terrorist attacks. Nearly 75 percent of the experts (32 of 43) identified one or more components of the distribution system. In fact, more experts identified the distribution system as the single most important vulnerability (12 of 43) of all system components. The other physical assets most frequently cited were source water supplies, critical information systems, and chemicals that are stored on site for use in the treatment process. Importantly, the experts also identified overarching vulnerability issues that may involve multiple system components, or even an entire drinking water system. Chief among these issues were (1) a lack of redundancy in vital systems, which increases the likelihood that an attack could render a system inoperable; and (2) the difficulty many systems face due to a lack of information on the most serious threats to which they are exposed. In general, the panelists' observations were similar to those of major public and private organizations that have assessed the vulnerability of these systems to terrorist attacks, including the National Academy of Sciences, Sandia National Laboratories, and key industry associations.

- About 90 percent of the experts agreed "strongly" or "somewhat" that allocation decisions should be based on assessments of drinking water utilities' vulnerabilities, which the utilities are required to prepare by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. In addition, the experts favored funding priority for utilities serving high-density populations, with over 90 percent indicating that they deserve at least a "high" priority and over 50 percent indicating they deserve "highest" priority. Utilities serving critical assets (such as military bases and other sensitive government facilities, national icons, and key cultural or academic institutions) were also recommended as high-

priority recipients. When asked to identify the most effective mechanisms for distributing these federal funds to recipients, over half the experts indicated that direct federal grants would be "very effective" in doing so. Many also favored including a requirement for matching funds as a grant condition. Some experts also recommended using the Drinking Water State Revolving Fund (DWSRF) for this purpose, particularly to support upgrades that need to be implemented quickly.

- When asked to identify and set priorities for security-enhancing activities most deserving of federal support, the experts most frequently identified activities that fell into three broad categories:

    - *Physical and technological improvements*—needed for both physical alterations to improve the security of drinking water systems, and for the development of technologies to prevent, detect, or respond to an attack. The need to develop near real-time monitoring technologies, which would be particularly useful in quickly detecting contaminants in water that has already left the treatment plant for the consumer, had by far the strongest support.

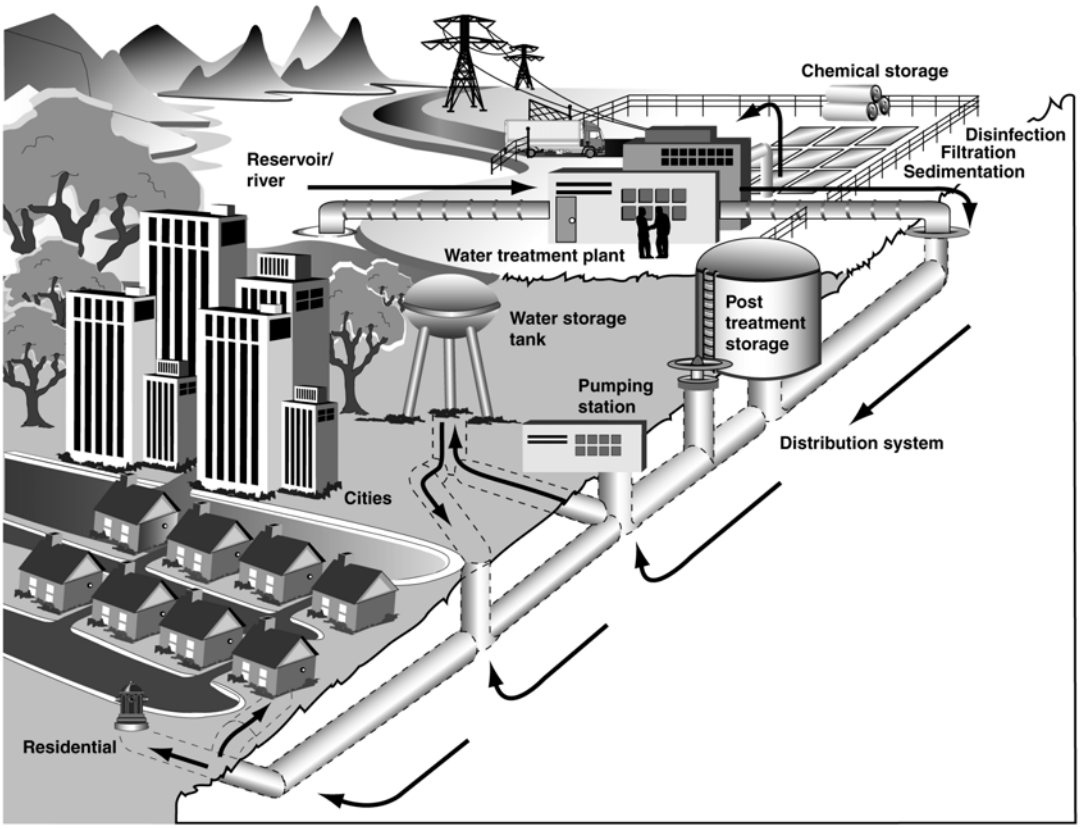
    - *Education and training*—to be provided to both utility and nonutility personnel responsible for preventing, responding to, and recovering from an attack. These activities include, among other things, support for simulation exercises to provide responders with experience in carrying out utilities' emergency response plans; specialized training of utility personnel responsible for security; general training of utility personnel to augment security awareness among all staff; and multidisciplinary consulting teams to independently analyze utilities' security preparedness and recommend security-related improvements.

- *Strengthened operational relationships*—especially between water utilities and other agencies (public health agencies, enforcement agencies, and neighboring utilities, among others) that may have key roles in an emergency response. This category also includes developing common protocols to engender a consistent approach among utilities in detecting and diagnosing threats, and the testing of local emergency response systems to ensure that participating agencies coordinate their actions effectively.

Background

Drinking water systems vary by size and other factors, but as illustrated in figure 1, they most typically include a supply source, treatment facility, and distribution system. A water system's supply source may be a reservoir, aquifer, or well, or a combination of these sources. Some systems may also include a dam to help maintain a stable water level, and aqueducts and transmission pipelines to deliver the water to a distant treatment plant. The treatment process generally uses filtration, sedimentation, and other processes to remove impurities and harmful agents, and disinfection processes such as chlorination to eliminate biological contaminants. Chemicals used in these processes, most notably chlorine, are often stored on site at the treatment plant. Distribution systems comprise water towers, piping grids, pumps, and other components to deliver treated water from treatment systems to consumers. Particularly among larger utilities, distribution systems may contain thousands of miles of pipes and numerous access points.

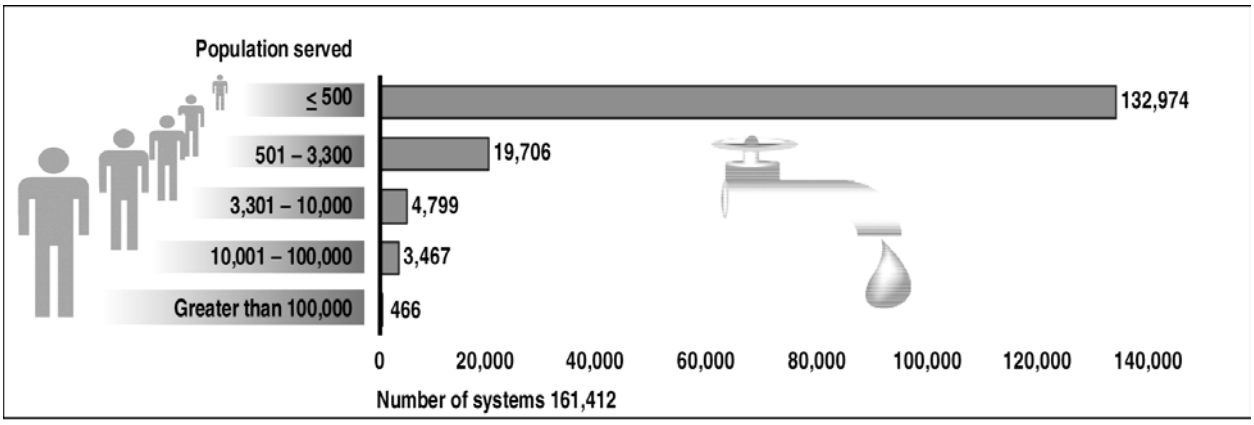
Figure 1: Key Components of a Typical Drinking Water System



Source: GAO.

Nationwide, there are more than 160,000 public water systems that individually serve from as few as 25 people to 1 million people or more. As figure 2 illustrates, nearly 133,000 of these water systems serve 500 or fewer people. Only 466 systems serve more than 100,000 people each, but these systems, located primarily in urban areas, account for early half of the total population served.

Figure 2: Number of Drinking Water Systems That Serve Various Populations



Source: GAO.

Until the 1990s, emergency planning at drinking water utilities generally focused on responding to natural disasters and, in some cases, domestic threats such as vandalism. In the 1990s, however, both government and industry officials broadened the process to account for terrorist threats. Among the most significant actions taken was the issuance in 1998 of Presidential Decision Directive 63 to protect the nation's critical infrastructure against criminal and terrorist attacks. The directive designated the Environmental Protection Agency (EPA) as the lead federal agency to address the water infrastructure and to work with both public and private organizations to develop emergency preparedness strategies. EPA, in turn, appointed the Association of Metropolitan Water Agencies to coordinate the water industry's role in emergency preparedness. During this time, this public-private partnership focused primarily on cyber security threats for the several hundred community water systems that each served over 100,000 persons. The partnership was broadened in 2001 to include both the drinking water and wastewater sectors, and focused on systems serving more than 3,300 people.

Efforts to better protect drinking water infrastructure were accelerated dramatically after the September 11 attacks. EPA and the drinking water industry launched efforts to share information on terrorist threats and response strategies. They also undertook initiatives to develop guidance and training programs to assist utilities in identifying their systems' vulnerabilities. As a major step in this regard, EPA supported the development,

by American Water Works Association Research Foundation and Sandia National Laboratories, of a vulnerability assessment methodology for larger drinking water utilities. The push for vulnerability assessments was then augmented by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act). Among other things, the act required each community water system serving more than 3,300 individuals to conduct a detailed vulnerability assessment by specified dates in 2003 or 2004, depending on their size.

Since we issued our report in October, several Homeland Security Presidential Directives (HSPDs) were issued that denote new responsibilities for EPA and the water sector. HSPD 7 designates EPA as the water sector's agency specifically responsible for infrastructure protection activities, including developing a specific water sector plan for the National Infrastructure Protection Plan that the Department of Homeland Security must produce. HSPD 9 directs EPA to develop a surveillance and monitoring program to provide early warning in the event of a terrorist attack using diseases, pests, or poisonous agents. EPA is also charged, under HSPD 9, with developing a nationwide laboratory network to support the routine monitoring and response requirements of the surveillance program. HSPD 10 assigns additional responsibilities to EPA for decontamination efforts.

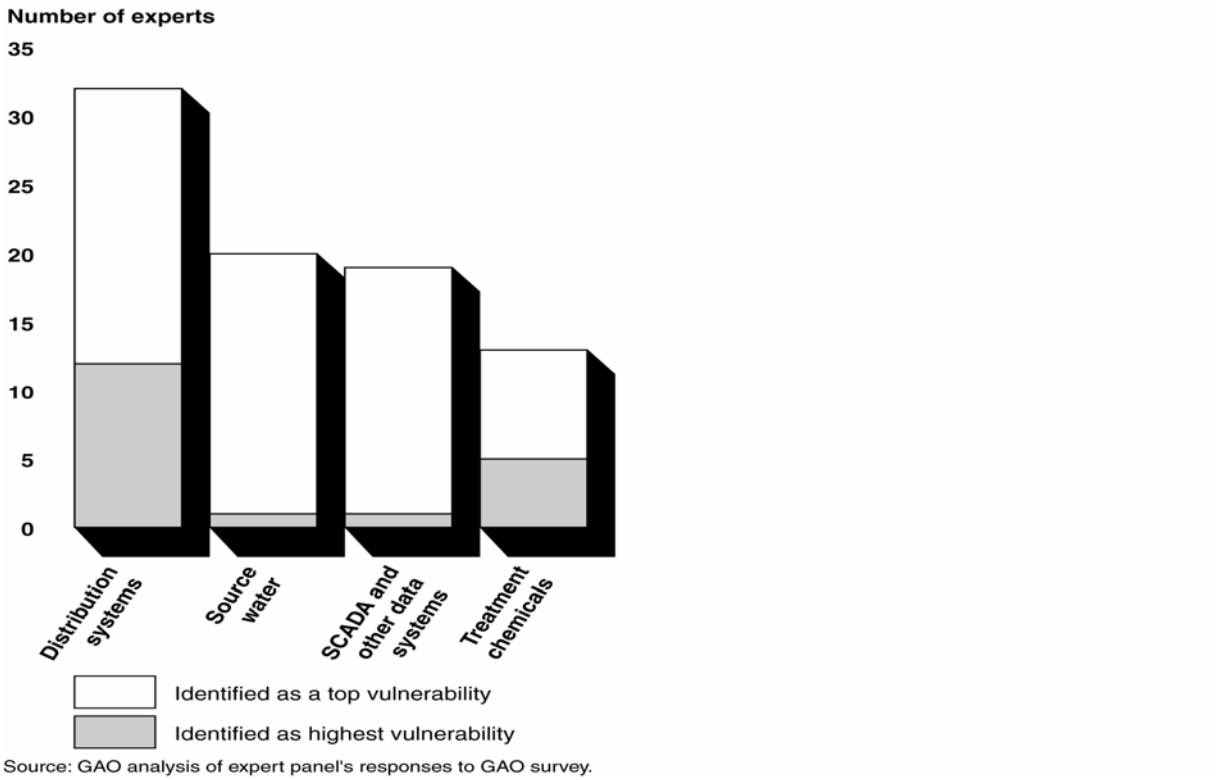
To obtain information for our analysis, we conducted a three-phase, Web-based survey of 43 experts on drinking water security. In identifying these experts, we sought to achieve balance in terms of area of expertise (i.e., state and local emergency response, engineering, epidemiology, public policy, security and defense, drinking water treatment, risk assessment and modeling, law enforcement, water infrastructure, resource economics, bioterrorism, public health, and emergency and crisis management). In addition, we attempted to achieve participation by experts from key federal organizations, state and local agencies, industry and nonprofit organizations, and water utilities serving populations of varying sizes. To obtain information from the expert panel, we employed a modified version of the Delphi method. The Delphi method is a systematic process for obtaining individuals' views and seeking consensus among them,

if possible, on a question or problem of interest. Since first developed by the RAND Corporation in the 1950s, the Delphi method has generally been implemented using face-to-face group discussions. For this study, however, we administered the method through the Internet. We conducted our work in accordance with generally accepted government auditing standards between July 2002 and August 2003.

Experts Identified Key Vulnerabilities That Could Compromise Drinking Water Systems' Security

Our panel of experts identified several key physical assets of drinking water systems as the most vulnerable to intentional attack. In general, their observations were similar to those of public and private organizations that have assessed the vulnerability of these systems to terrorist attacks, including the National Academy of Sciences, Sandia National Laboratories, and key industry associations. In particular, as shown in figure 3, nearly 75 percent of the experts (32 of 43) identified the distribution system or its components as among the top vulnerabilities of drinking water systems. Experts also identified overarching issues compromising how well these assets are protected. Chief among these issues are (1) a lack of redundancy in vital systems, which increases the likelihood that an attack could render a system inoperable; and (2) the difficulty many systems face in understanding the nature of the threats to which they are exposed.

Figure 3: Key Vulnerabilities Identified As Compromising Drinking Water Systems' Security



Source: GAO analysis of expert panel's responses to GAO survey.

I would first like to discuss the distribution system, since it was cited most frequently as a key vulnerability by our panelists. The distribution system delivers drinking water primarily through a network of underground pipes to homes, businesses, and other customers. While the distribution systems of small drinking water utilities may be relatively simple, larger systems serving major metropolitan areas can be extremely complex. One such system, for example, measures water use through 670,000 metered service connections, and distributes treated water through nearly 7,100 miles of water mains that range from 2 inches to 10 feet in diameter. In addition to these pipelines and connections, other key distribution system components typically include numerous pumping stations, treated water storage tanks, and fire hydrants.

In highlighting the vulnerability of distribution systems, our panelists most often cited their accessibility at so many points. One expert, for example, cited the difficulty in preventing the introduction of a contaminant into the distribution system from inside a

building "regardless of how much time, money, or effort we spend protecting public facilities." Experts also noted that since the water in the distribution system has already been treated and is on the way to the consumer, the distribution of a chemical, biological, or radiological agent in such a manner would be virtually undetectable until it was too late to prevent harm. While research on the fate and transport of contaminants within water treatment plants and distribution systems is under way, according to one expert, limited technologies are readily available that can detect a wide range of contaminants once treated water is released through the distribution system for public use.

Several other components, though not considered as critical as the distribution system, were still the subject of concern. Nearly half the experts (20 of 43) identified source water as among drinking water systems' top vulnerabilities. One expert noted, for example, that "because of the vast areas covered by watersheds and reservoirs, it is difficult to maintain security and prevent intentional or accidental releases of materials that could have an adverse impact on water quality." Yet some experts cited factors that mitigate the risks associated with source water, including (1) the source water typically involves a large volume of water, which in many cases could dilute the potency of contaminants; (2) the length of time (days or even weeks) that it typically takes for source water to reach consumers; and (3) the source water will go through a treatment process in which many contaminants are removed.

Also cited as vulnerabilities were the sophisticated computer systems that drinking water utilities have come to rely upon to manage key functions. These Supervisory Control and Data Acquisition (SCADA) systems allow operators to monitor and control processes throughout their drinking water systems. Although SCADA systems have improved water utilities' efficiency and reduced costs, almost half of the experts on our panel (19 of 43) identified them as among these utilities' top vulnerabilities.

Thirteen of the 43 experts identified treatment chemicals, particularly chlorine used for disinfection, as among utilities' top vulnerabilities. Experts cited the inherent danger of

storing large cylinders of a chemical on site, noting that their destruction could release toxic gases in densely populated areas. Some noted, however, that this risk has been alleviated by utilities that have chosen to use the more stable liquid form of chlorine instead of the more vulnerable compressed gas canisters that have traditionally been used.

Finally, experts identified overarching issues that compromise the integrity of multiple physical assets, or even the entire drinking water system. Among these is the lack of redundancy among vital systems. Many drinking water systems are "linear"—that is, they have single transmission lines leading into the treatment facility and single pumping stations along the system, and often use a single computer operating system. They also depend on the electric grid, transportation systems, and single sources of raw materials (e.g., treatment chemicals). Many experts expressed concern that problems at any of these "single points of failure" could render a system inoperable unless redundant systems are in place. Experts also cited the lack of sufficient information to understand the most significant threats confronting individual utilities. According to the American Water Works Association, assessments of the most credible threats facing a utility should be based on knowledge of the "threat profile" in its specific area, including information about past events that could shed light on future risks. Experts noted, however, that such information has been difficult for utilities to obtain. One expert suggested that the intelligence community needs to develop better threat information and share it with the water sector.

Experts' Views on the Allocation and Distribution of Federal Funds

Many drinking water utilities have been financing at least some of their security upgrades by passing along the costs to their customers through rate increases. Given the cost of these upgrades, however, the utility industry is also asking that the taxpayer shoulder some of the burden through the appropriations process. Should Congress and the administration agree to this request, they will need to address key issues concerning who

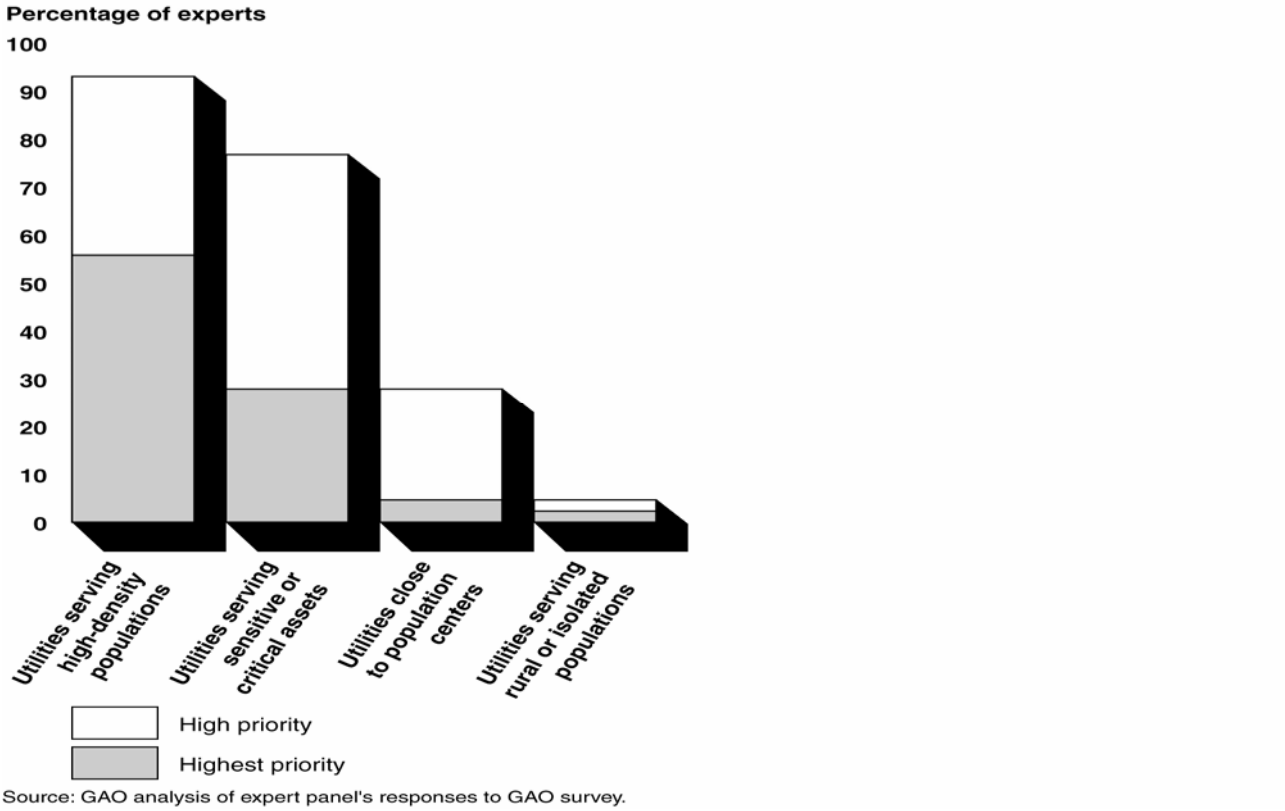
should receive the funds and how they should be distributed. With this in mind, we asked our panel of experts to focus on the following key questions: (1) To what extent should utilities' vulnerability and risk assessment information be considered in making allocation decisions? (2) What types of utilities should receive funding priority? and (3) What are the most effective mechanisms for directing these funds to recipients?

Regarding the first of these questions, about 90 percent of the experts (39 of 43) agreed "strongly" or "somewhat" that funds should be allocated on the basis of vulnerability assessment information, with some citing the vulnerability assessments (VAs) required by the Bioterrorism Act as the best available source of this information. Several experts, however, pointed to a number of complicating factors. Perhaps the most significant constraint is the Bioterrorism Act's provision precluding the disclosure of any information that is "derived" from vulnerability assessments submitted to EPA. The provision protects sensitive information about each utility's vulnerabilities from individuals who may then use the information to harm the utility. Hence, the law specifies that only individuals designated by the EPA Administrator may have access to the assessments and related information. Yet, according to many of the experts, even those individuals may face constraints in using the information. They may have difficulty, for example, in citing vulnerability assessments to support decisions on allocating security-related funds among utilities, as well as decisions concerning research priorities and guidance documents. Others cited an inherent dilemma affecting *any* effort to set priorities for funding decisions based on the greatest risk—whatever does not receive attention becomes a more likely target.

Regarding the second question concerning the types of utilities that should receive funding priority, 93 percent of the experts (40 of 43) indicated that utilities serving high-density population areas should receive a high or the highest priority in funding (See figure 4.). Fifty-five percent deemed this criterion as the highest priority. Most shared the view of one expert who noted that directing limited resources to protect the greatest number of people is a common factor when setting funding priorities. Experts also assigned high priority to utilities serving critical assets, such as national icons

representing the American image, military bases, and key government, academic, and cultural institutions.

Figure 4: Experts' Views on Which Types of Water Utilities Should Receive Priority for Federal Funds

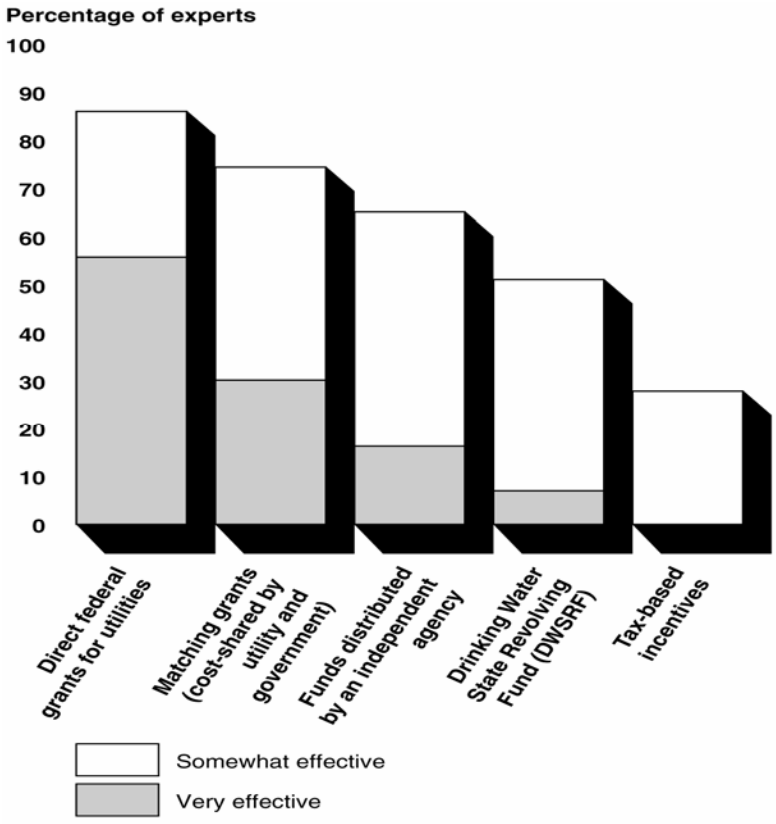


Source: GAO analysis of expert panel's responses to GAO survey.

At the other end of the spectrum, only about 5 percent of the experts (2 of 43) stated that utilities serving rural or isolated populations should receive a high or highest priority for federal funding. These two panelists commented that such facilities are least able to afford security enhancements and are therefore in greatest need of federal support. Importantly, the relatively small percentage of experts advocating priority for smaller systems may not fully reflect the concern among many of the experts for the safety of these utilities. For example, several who supported higher priority for utilities serving high-density populations cautioned that while problems at a large utility will put more people at risk, utilities serving small population areas may be more vulnerable because of weaker treatment capabilities, fewer highly trained operators, and more limited resources.

Regarding the mechanisms for distributing federal funds, 86 percent of the experts (37 of 43) indicated that direct grants would be "somewhat" or "very" effective in allocating federal funds (See figure 5.) One expert cited EPA's distribution of direct security-related grant funds in 2002 to larger systems to perform their VAs as a successful initiative. Importantly, 74 percent also supported a matching requirement for such grants as somewhat or very effective. One expert pointed out that such a requirement would effectively leverage limited federal dollars, thereby providing greater incentive to participate.

Figure 5: Recommended Approaches to Distribute Federal Funds



Source: GAO analysis of expert panel's responses to GAO survey.

The Drinking Water State Revolving Fund (DWSRF) received somewhat less support as a mechanism for funding security enhancements. About half of the experts (22 of 43) indicated that the fund would be somewhat or very effective in distributing federal funds,

but less than 10 percent indicated that it would be very effective.[1] One expert cautioned that the DWSRF should be used only if a process were established that separated funding for security-related needs from other infrastructure needs. Others stated that as a funding mechanism, the DWSRF would not be as practical as other mechanisms for funding improvements requiring immediate attention, but would instead be better suited for longer-term improvements.

Activities Experts Identified as Most Deserving of Federal Support

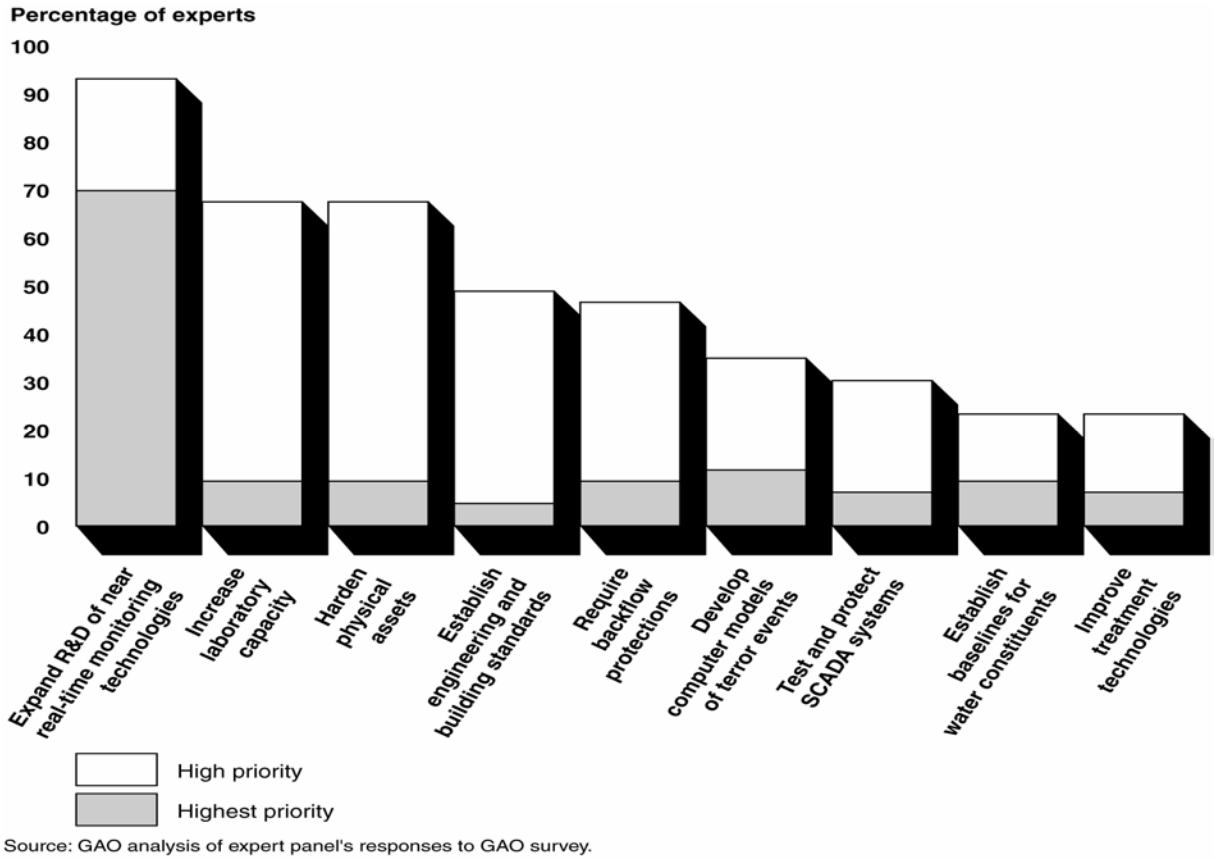
When experts were asked to identify specific security-enhancing activities most deserving of federal support, their responses generally fell into three categories: (1) *physical and technological upgrades* to improve security and research to develop technologies to prevent, detect, or respond to an attack, (2) *education and training* to support, among other things, simulation exercises to provide responders with experience in carrying out emergency response plans, and specialized training of utility security staff; and (3) *strengthening key relationships* between water utilities and other agencies that may have key roles in an emergency response, such as public health agencies, law enforcement agencies, and neighboring drinking water systems.

As illustrated in figure 6, specific activities to enhance physical security and support technological improvements generally fell into nine subcategories. Of these, the development of "near real-time monitoring technologies," capable of providing near real-time data for a wide array of potentially harmful water constituents, received far more support for federal funding than any other subcategory—over 93 percent of the experts (40 of 43) rated this subcategory as deserving at least a high priority for federal funding. More significantly, almost 70 percent (30 of 43) rated it the highest priority—far surpassing the rating of any other category. These technologies were cited as critical in

[1] The DWSRF program provides federal grant funds to states, which in turn allow the states to help public water systems in their efforts to protect public health and ensure their compliance with the Safe Drinking Water Act. States may use the funds to provide loans to public water systems, and may reserve a portion of their grants to finance other projects that protect sources of drinking water and enhance the technical, financial, and managerial capacity of public water systems.

efforts to quickly detect contamination events, minimize their impact, and restore systems after an event has passed. The experts' views were consistent with those of the National Academies of Science, which in a 2002 report highlighted the need for improved monitoring technologies as one of four highest-priority areas for drinking water research and development.[2] The report noted that such technologies differ significantly from those currently used for conventional water quality monitoring, stating further that sensors are needed for "better, cheaper, and faster sensing of chemical and biological contaminants."

Figure 6: Activities Identified by Expert Panel to Enhance Physical Security and Support Technological Improvements



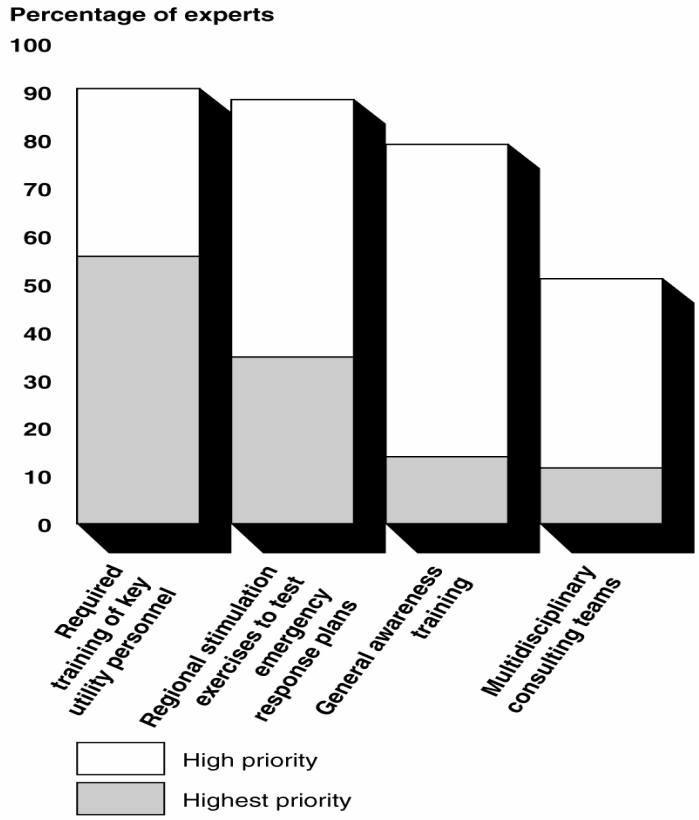
Source: GAO analysis of expert panel's responses to GAO survey.

[2] *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, p. 250. The National Research Council of the National Academies. (Washington, D.C.: The National Academies Press, 2002).

In addition to real-time monitoring technologies, the experts voiced strong support for (1) increasing laboratories' capacity to deal with spikes in demand caused by chemical, biological, or radiological contamination of water supplies, and (2) "hardening" the physical assets of drinking water facilities through improvements such as adding or repairing fences, locks, lighting systems, and cameras and other surveillance equipment. Regarding the latter of these two, however, some experts cited inherent limitations in attempting to comprehensively harden a drinking water facility's assets. In particular, they noted in particular that, unlike nuclear power or chemical plants, a drinking water system's assets are spread over large geographic areas, particularly the source water and distribution systems.

Regarding efforts to improve education and training, over 90 percent of the experts (39 of 43) indicated that improved technical training for security-related personnel warrants at least a high priority for federal funding. (See figure 7.) Over 55 percent (24 of 43) indicating that it deserved the highest priority. To a lesser extent, experts supported general training for other utility personnel to increase their awareness of security issues. The panelists also underscored the importance of conducting regional simulation exercises to test emergency response plans, with more than 88 percent (38 of 43) rating this as a high or highest priority for federal funding. Such exercises are intended to provide utility and other personnel with the training and experience needed both to perform their individual roles in an emergency and to coordinate these roles with other responders. Finally, about half the experts assigned at least a high priority to supporting multidisciplinary consulting teams ("Red Teams"), comprising individuals with a wide array of backgrounds, to provide independent analyses of utilities' vulnerabilities.

Figure 7: Activities Identified by Experts to Improve Education and Training

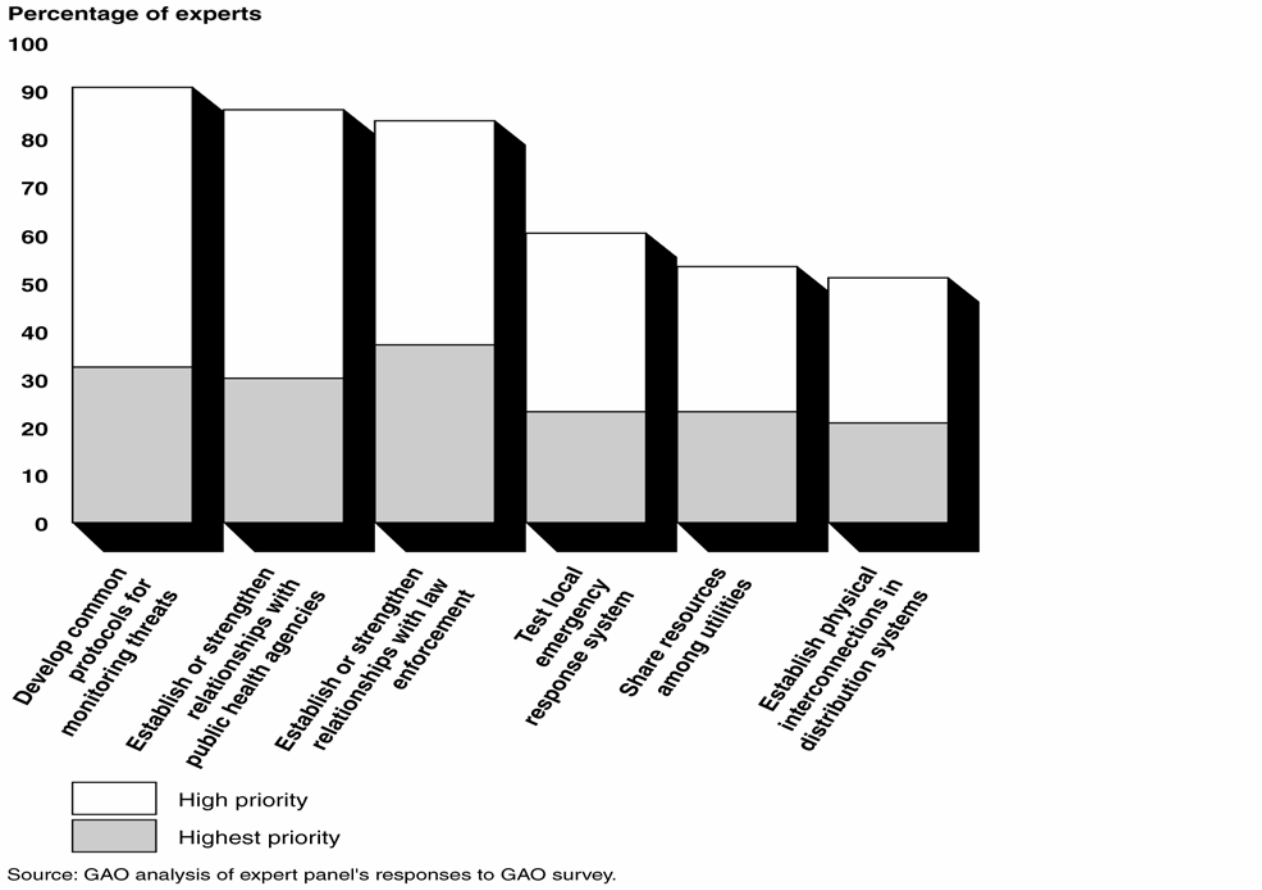


Source: GAO analysis of expert panel's responses to GAO survey.

As illustrated in figure 8, experts also cited the need to improve cooperation and coordination between drinking water utilities and certain other organizations as key to improving utilities' security. Among the organizations most often identified as critical to this effort are public health and law enforcement agencies, which have data that can help utilities better understand their vulnerabilities and respond to emergencies. In addition, the experts cited the value of utilities' developing mutual aid arrangements with neighboring utilities. Such arrangements sometimes include, for example, sharing back-up power systems or other critical equipment. One expert described an arrangement in the San Francisco Bay Area—the Bay Area Security Information Collaborative (BASIC)—in which eight utilities meet regularly to address security-related topics. Finally, over 90 percent of the experts (39 of 43) rated the development of common protocols among drinking water utilities to monitor drinking water threats as warranting a high or highest priority for federal funding. Drinking water utilities vary widely in how

they perceive threats and detect contamination, in large part because few common protocols exist that would help promote a more consistent approach toward these critical functions. Some experts noted, in particular, the need for protocols to guide the identification, sampling, and analysis of contaminants.

Figure 8: Activities Identified by Experts to Strengthen Relationships Among Agencies and Utilities



Source: GAO analysis of expert panel's responses to GAO survey.

Observations

In 2002, EPA's Strategic Plan on Homeland Security set forth the goal of significantly reducing unacceptable security risks at water utilities across the country by completing appropriate vulnerability assessments; designing security enhancement plans; developing emergency response plans; and implementing security enhancements. The plan further

committed to providing federal resources to help accomplish these goals as funds are appropriated.

Key judgments about which recipients should get funding priority, and how those funds should be spent, will have to be made in the face of great uncertainty about the likely targets of attacks, the nature of attacks (whether physical, cyber, chemical, biological, or radiological), and the timing of attacks. The experts on our panel have had to consider these uncertainties in developing their own judgments about these issues. These judgments, while not unanimous on all matters, suggested a high degree of consensus on a number of key issues.

We recognize that such sensitive decisions must ultimately take into account political, equity, and other considerations. But we believe they should also consider the judgments of the nation's most experienced individuals regarding these matters, such as those included on our panel. It is in this context that we offer the results presented in this testimony as information for Congress and the administration to consider as they seek the best way to use limited financial resources to reduce threats to the nation's drinking water supply.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions you or other Members of this Subcommittee may have.

(360522)